Introduction to Windows 2000 Professional

The Windows 2000 operating system is a dynamic and continually changing operating system with new security patches and hot fixes being released often. In a normal production environment, it is highly recommended that you maintain a patching schedule to keep your systems up-to-date. For the purposes of this book, it is important that you do not patch your system. Because this system will be vulnerable to every exploit that has been discovered since Windows 2000 was first released, it is extremely important that you do not connect it to a production network. Several patches will cause issues when completing various labs in this book. By following the installation guide, you are assured of getting the maximum value out of the activities covered throughout this book.

This "Introduction to Windows 2000 Professional" guide teaches you about the basic commands and actions you need to know for the NS 2003 Security Essentials Boot Camp. This document introduces you to the following: **cmd, ipconfig, regedit, regedt32, net use, netstat, cls, dir, mkdir, and the Task Manager.**

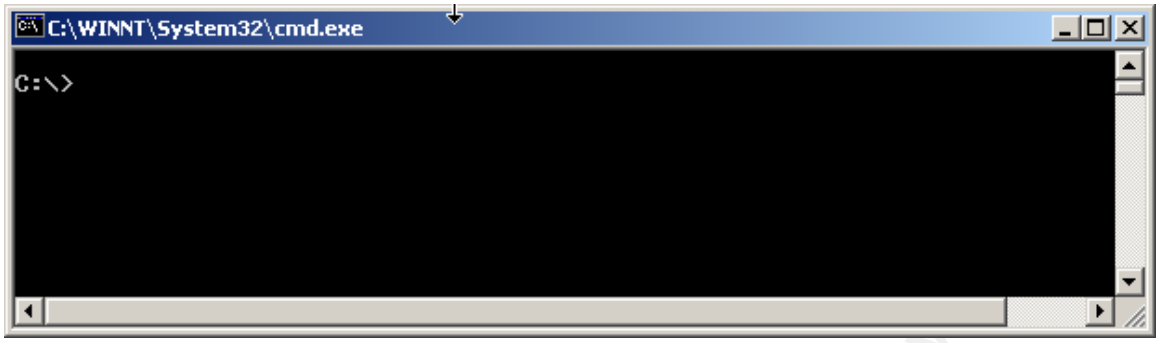
The 32-bit Cmd Prompt

Since the release of Windows 2000 Professional, the old 16-bit **command** window has been replaced with the 32-bit **cmd.** There are many benefits of using **cmd** including the following:

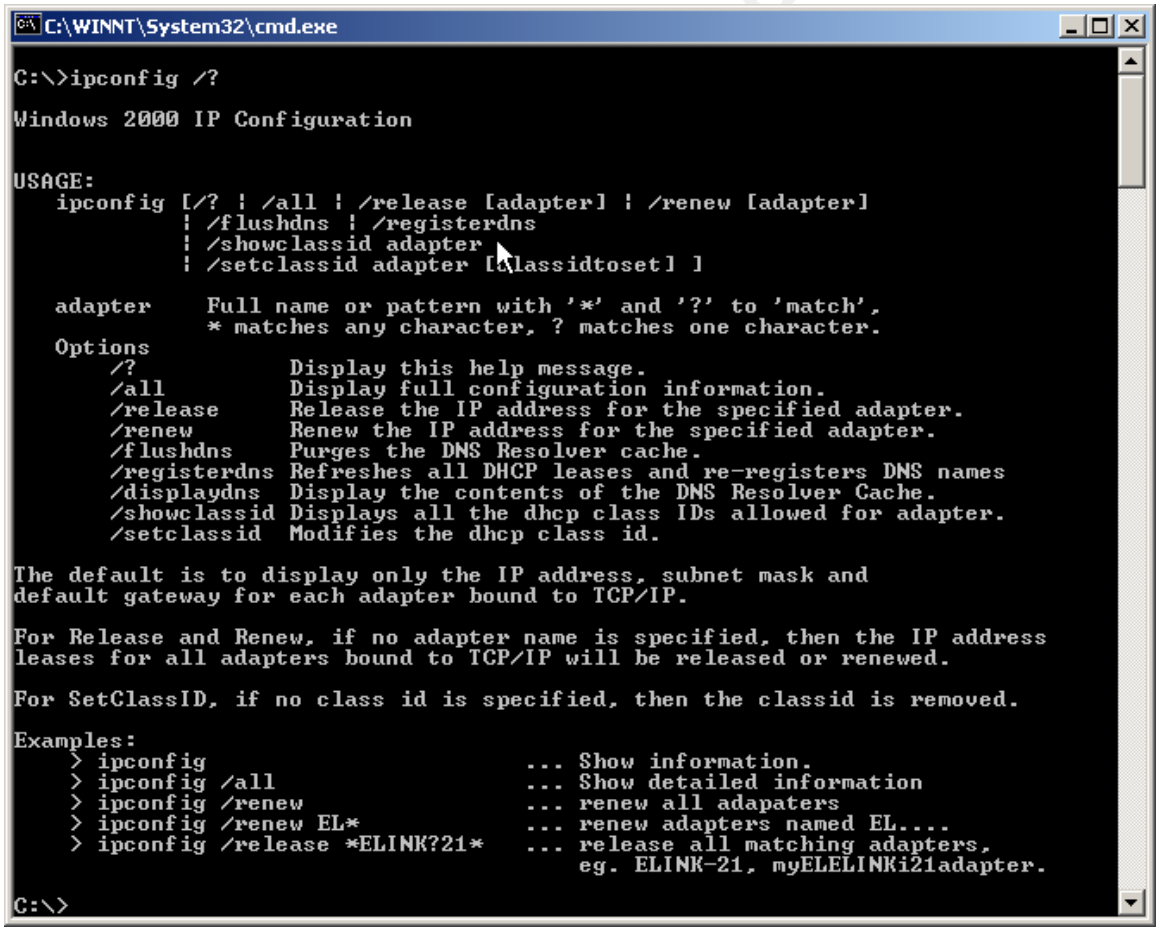
- The capability to run scripts in both the CMD language as well as the REXX language
- There are no 8.3 filename limitations
- The capability of running multiple commands on the same command line
- Support for command pipelines
- Help functionality with **/?**

The following list of tasks shows you how to use the command prompt to obtain help or information about your system:

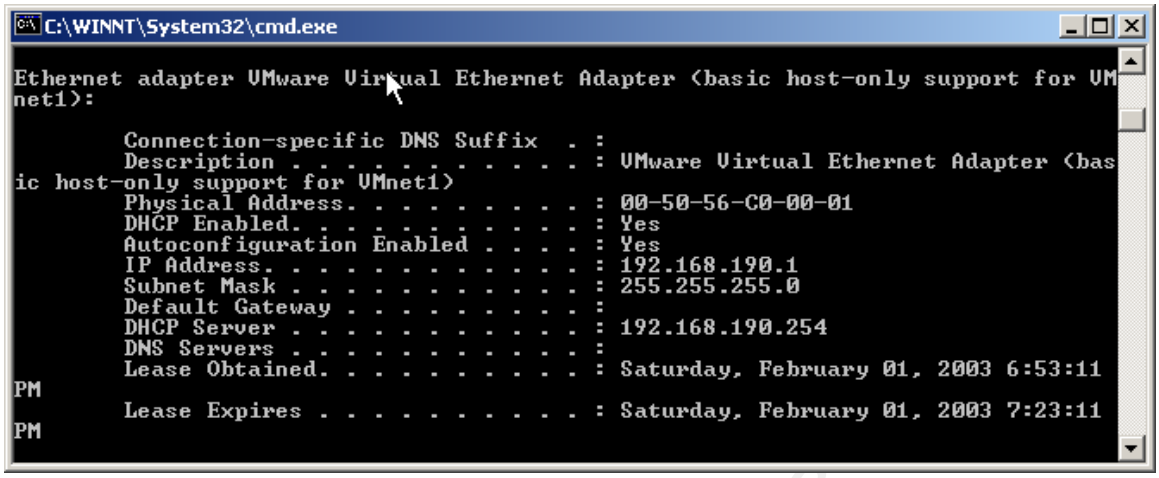
1. To display the command prompt, select **Start, Run**, and then type **cmd**. The following window appears.



2. If you need help with a command while using **cmd**, type **/?** after the command in question. To get NIC TCP/IP information, type **ipconfig**. To get a list of the available ipconfig options, type **ipconfig /?** after the command prompt, as shown in the following screen.



3. To get the IP address information for your system, type **ipconfig /all.** This also displays your MAC address, as shown in the following screen.



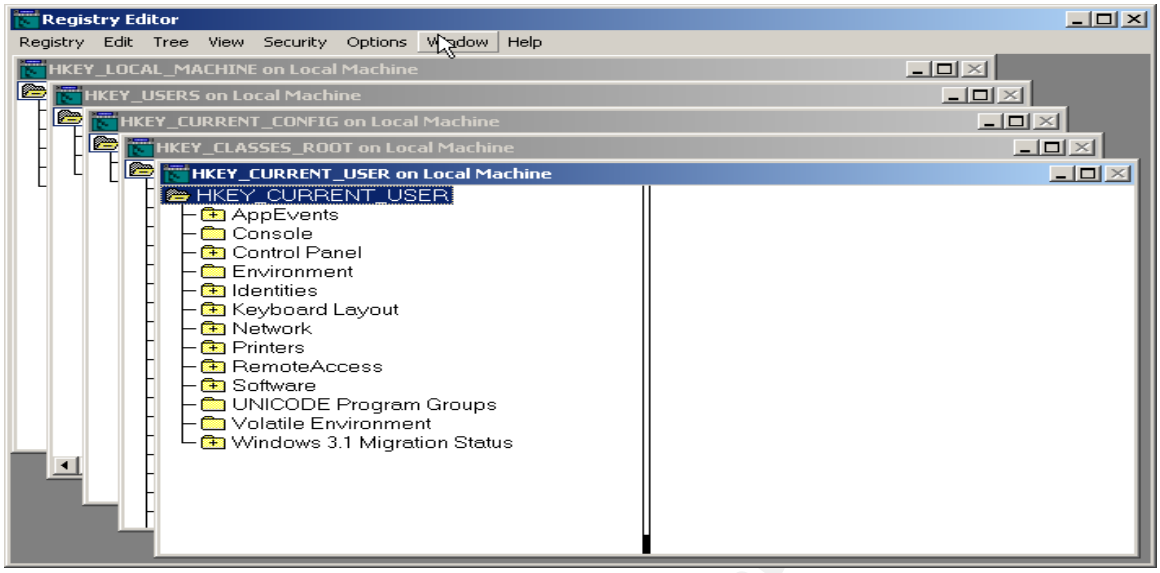
Editing the Registry

To edit the registry in a Windows environment you can use either the **regedit** or **regedt32** command at the Run prompt. When working in a Windows environment, I switch between the two commands depending on what I am doing. One of the nice features of using **regedit** versus **regedt32** is that you can search every hive for specific keys, values, and data. The **regedt32** command does not have a search feature. On the other hand, any value that has a *multi* value to it must be edited with the **regedt32** command. This section looks at both **regedit** and **regedt32,** so that you can see the differences between them.

Warning: When using **regedit** and **regedt32,** use caution because any change you make is permanent and could potentially render your system unusable.

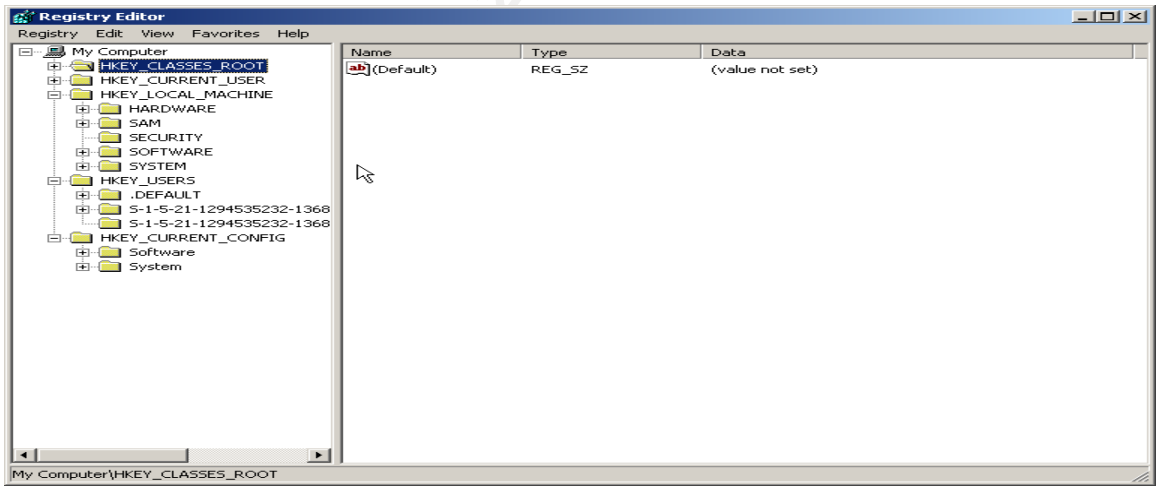
The following list of tasks explain how to edit the registry and how to use **regedt32**:

1. To start **regedt32**, choose **Start**, **Run**. Then, type **regedt32** and press **Enter**. The following is a screen shot of **regdt32**.



2. To ensure you can recover from making detrimental mistakes when editing the registry, you should always save a copy of the keys you change. To do this, choose **Registry, Save Key** and make a backup copy of the key.

   To start **regedit**, choose **Start, Run**, and then type **regedit.** Then, press **Enter**. The following screen shows an example of **regedit** (the Registry Editor).

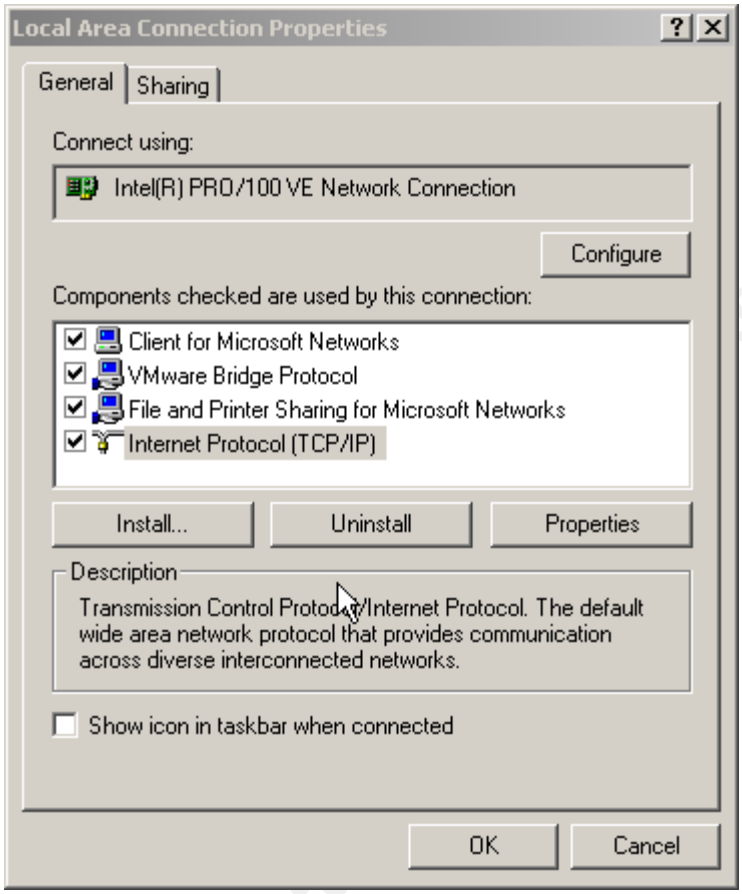


IP Changes

The following steps are necessary for making IP changes on your Windows 2000 Professional system:

1. To make IP address changes to your local machine, open the NIC properties. Open up your Control Panel by choosing **Start, Settings,**

Network and Dialup Settings. Highlight the local area connection. Right-click the Local Area Connection, and click **Properties.** The following screen appears.



2. Highlight **Internet Protocol (TCP/IP)** and click the **Properties** button.

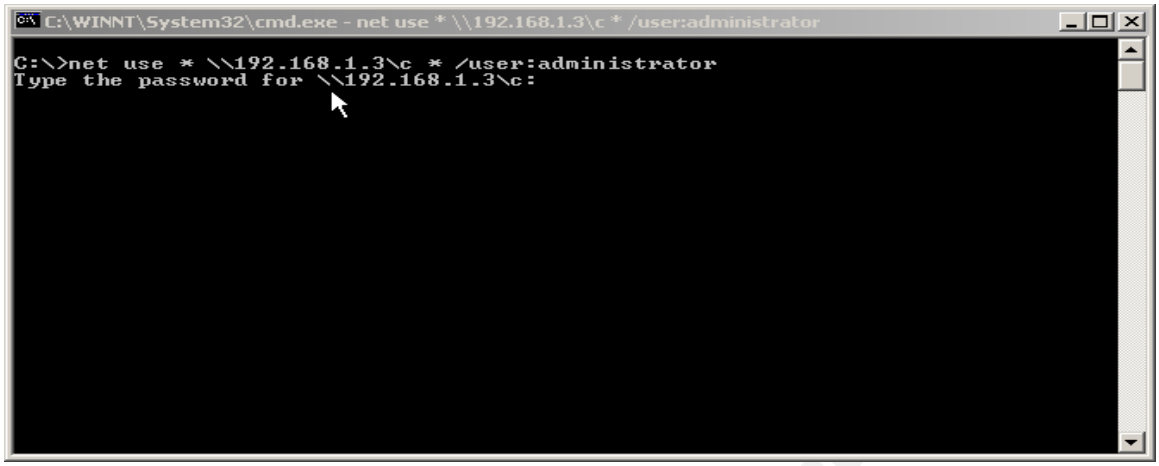
Connecting to Remote Devices

If you are like me, you don't want to browse to a remote device to connect to it. To make connections to remote devices without browsing to them, follow these steps:

1. Make a direct connection to a remote share by using the **net use** command. A typical **net use** command looks like this:

   Net use * \\<IP_ADDRESS>\<Share_Name * /user:<Remote_User_Name

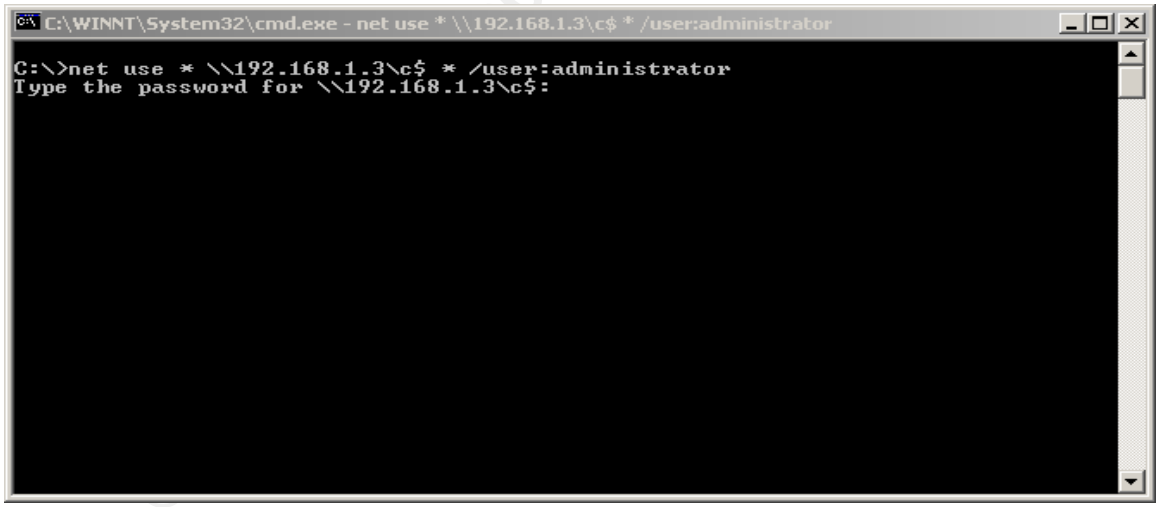
   Type the command after the prompt. Press **Enter**. You are prompted for a password, as shown in the following screen.



2. Even if a user does not explicitly share a folder or drive on his or her system, there are hidden administrator shares you can connect to if you happen to have the remote machine's Administrator password. Default administrative shares are as follows:

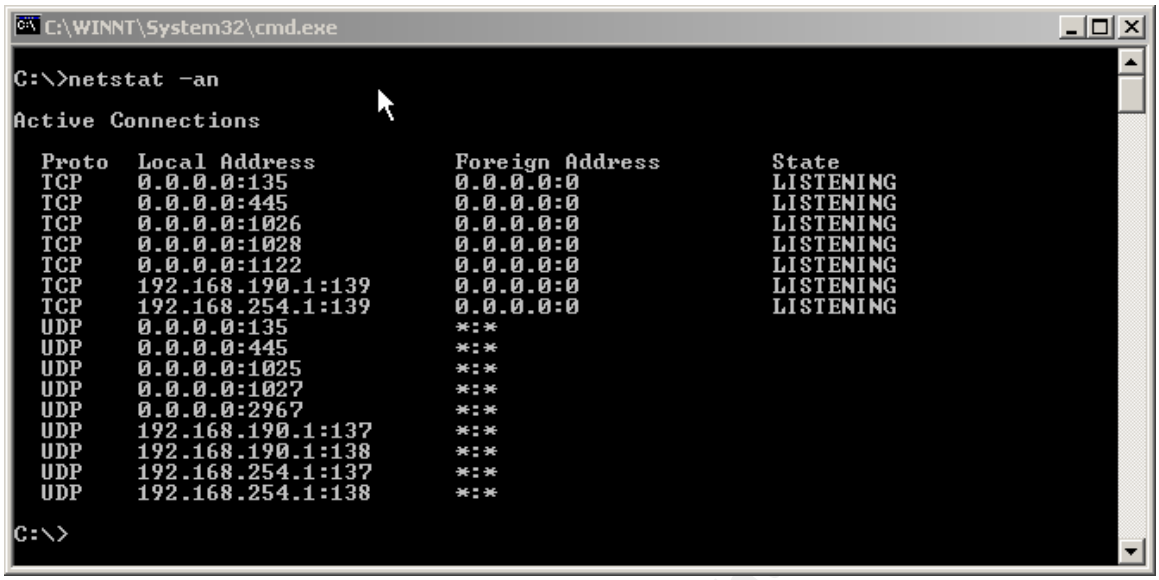
   C$, D$

   To connect to the **C$** or **D$** share, simply replace the share with the desired administrative share. The following screen shows how this was done for the share shown in the previous screen.



Viewing Ports

Throughout the exercises in this book, you are required to add services to your system. To see what ports are open on your boxand allow remote connections, you use the **netstat** command, as shown in the following screen.



You can see every open port and the state of each port. States include listening, waiting, or connected. The **netstat** command also shows you TCP and UDP connections.

Other Useful Commands

Some other commands to use at the cmd prompt are:

- **Cls—**Clears everything on the screen and returns you to the top of the **cmd** window
- **Dir**—Displays a directory listing
- **cd **—Returns you to c:\ from whatever directory you are in

Task Manager

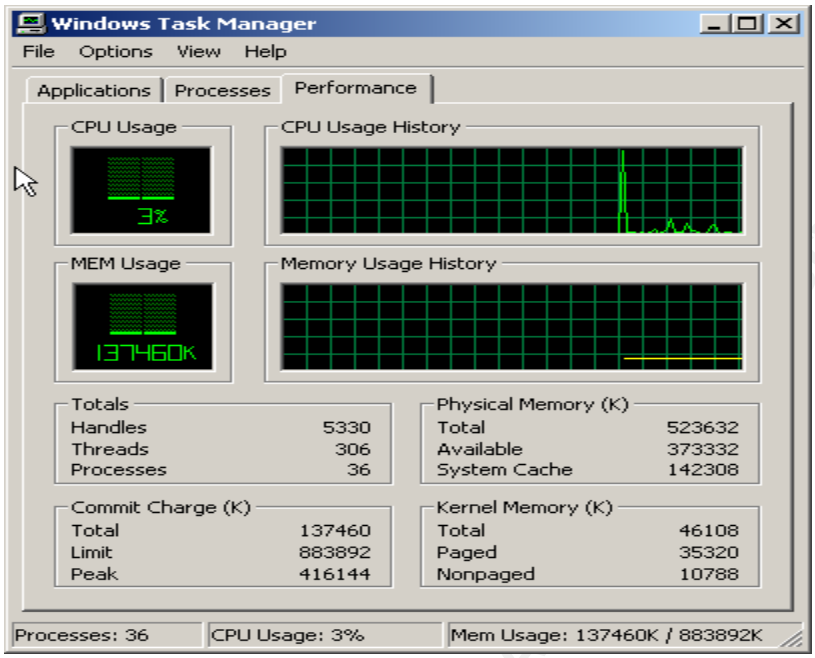
Another great built-in tool in Windows 2000 Professional is the Task Manager. The following list shows you how to open and use the Task Manager:

1. To open the Task Manager, right-click on the task bar and choose **Task Manager**. (The screen shot that follows step 2 shows the Task Manager's Performance tab.)

   Tip: Another way to open the Task Manager, which I recommend, is to hold down the **Ctrl, Shift,** and **Esc** keys simultaneously.

2. From this window, you can check the running processes on the device, the performance trends, and the applications that are currently running. It is a great tool to open if you have an application that stops responding. You can

open Task Manager, highlight the application, and then choose to close the offending application.



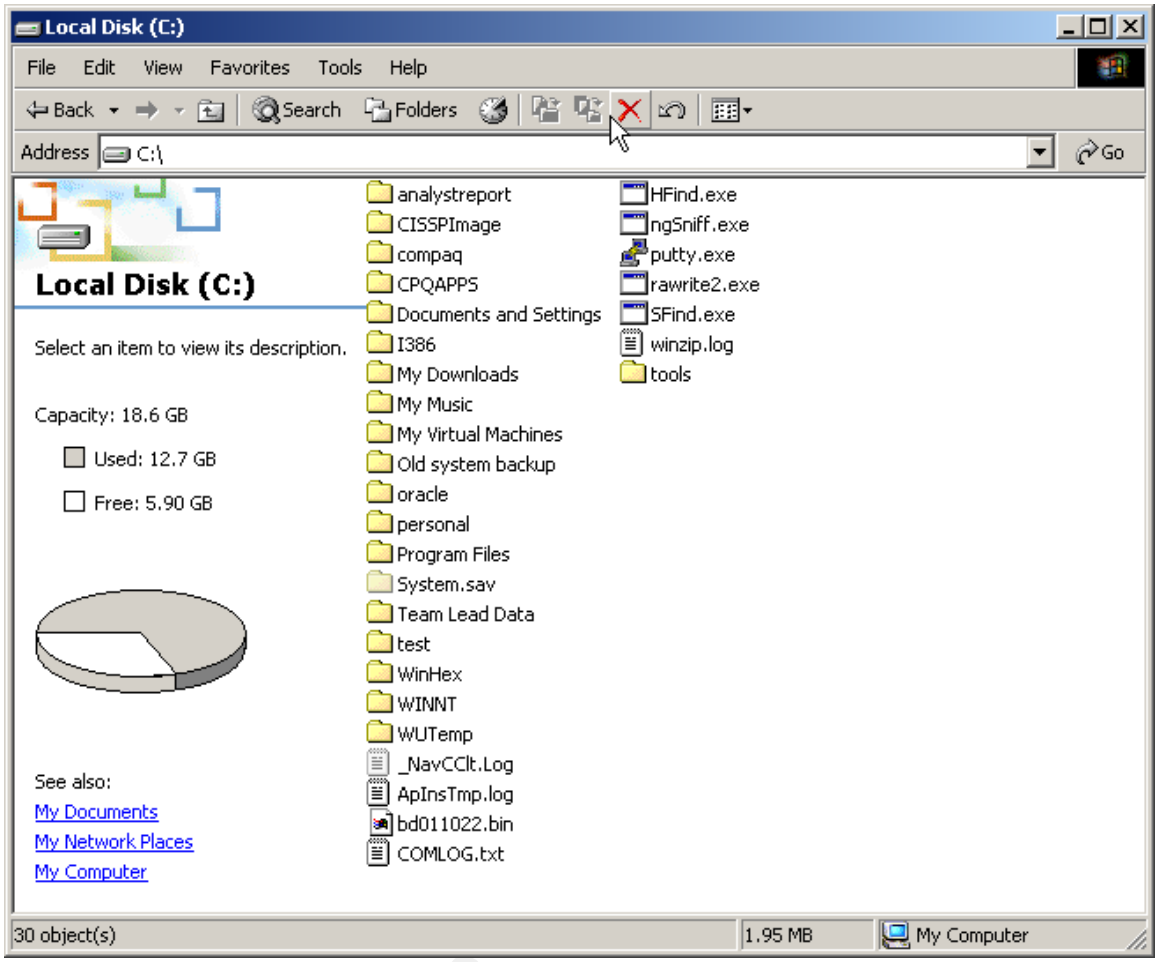
There are many other Windows 2000 Professional functions that are not covered in this book. Our goal is to give you the basics, so that you can quickly install and run the tools covered throughout the following chapters.

You should also note that contrary to popular belief, there are several tools and hack code that hackers and crackers can run from the Windows platform. The cool tools are not just reserved for the "*nix OS."

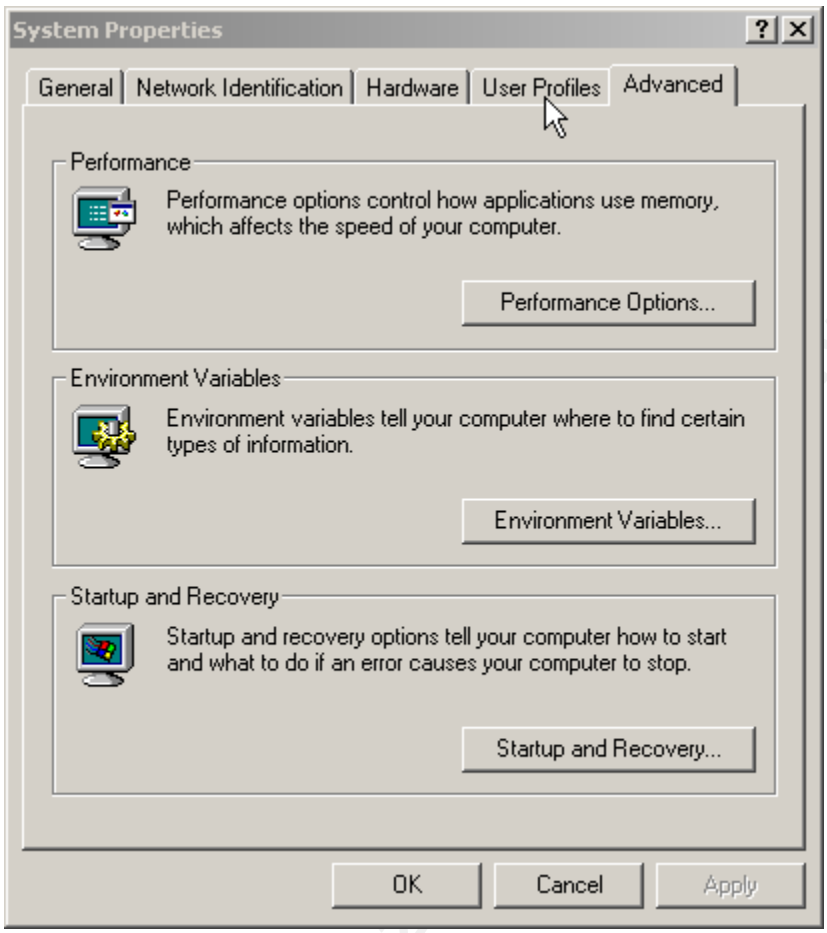
Setting Up the Directory Structure

Now that you have installed the operating system and seen some of the tools that are built into it, you need to set up your directory structure, so that it's consistent with the directory structure used for installing and storing the tools discussed in this book. Follow these steps to setup the directory structure:

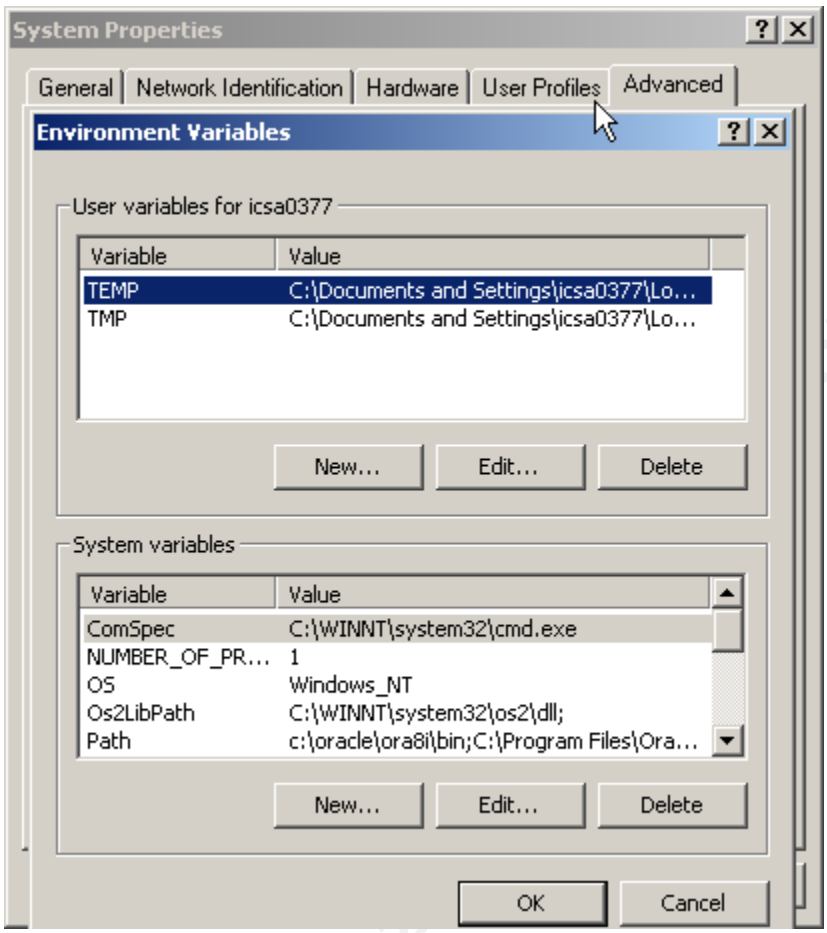
1. First double-click **My Computer** and then double-click **Local Disk (c:)**. The window that appears lists the structure of the **C:** drive. Right-click a spot in the window that is blank. Move your mouse down the menu that appears and left-click **New** and choose **Folder.** Name the folder **tools**. The following screen shows a directory structure with the new **tools** folder.



2. The exercises in this book require you to run several tools from the command line. Thus, you need to add the new folder we created, **c:\tools**, to PATH. If you do this, you won't have to navigate to the **tools** folder each time you want to run an application. To add the folder to PATH, right-click **My Computer.** Then, choose **Properties** from the pop-up menu. Click the **Advanced** tab, as shown in the following screen.



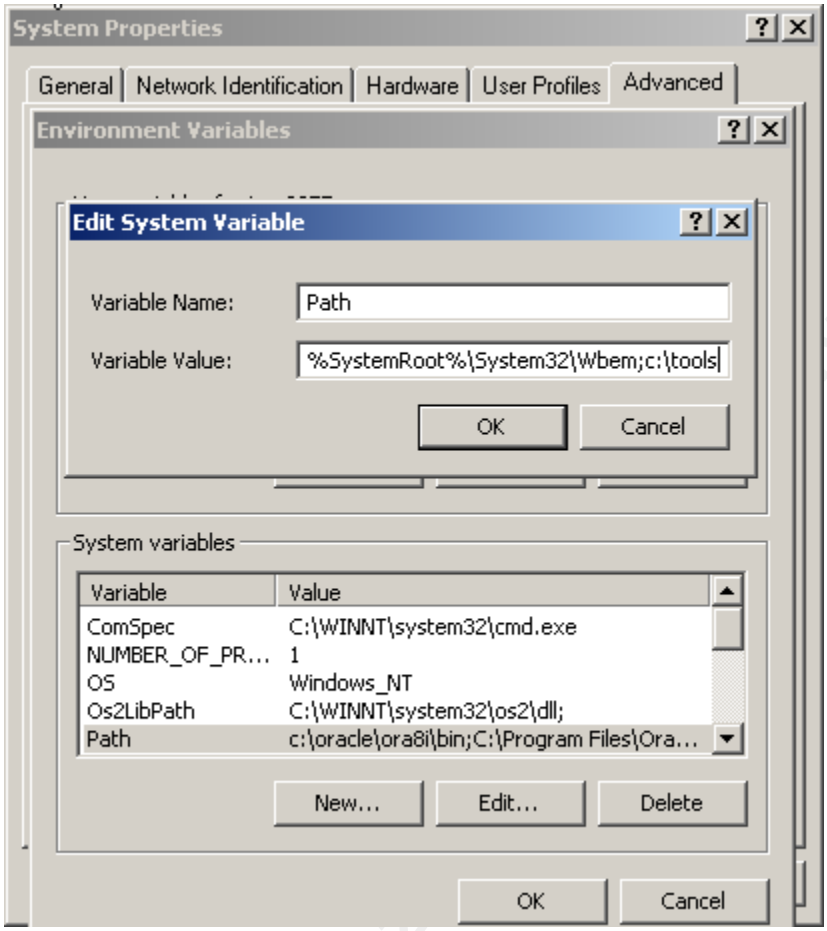
3. Click the **Environment Variables** button**.** In the **System Variables section,** highlight the line labeled **Path** and click **Edit**.



4. In the **Variable Value** field, move your cursor to the end of the line and add the following exactly as it is shown here:

   ;c:\tools

   Click **OK**.



The executables located in **c:\tools** can now be run from any directory in your file structure. This saves a lot of time when you are using command prompt and want to run an application from it.